สหัส พรหมสิทธิ์

เกณฑ์อาสาสมัครจากทั่วโลก เพื่อถอดรหัสที่ยากที่สุด

รู้จักคิดและรู้จักวางแผนระดมพล
ก็สามารถคิดการใหญ่เพื่อตีรหัส
ที่มีชื่อของโลกให้แตกได้
แม้ว่าจะใช้เวลานานนับเดือนก็ตาม

การล้วงความลับที่น่าจะสำคัญที่สุดเรื่องหนึ่งในโลกของคอมพิวเตอร์เน็ตเวอร์กก็คือการสามารถถอดรหัสพวกคีย์ต่าง ๆ เช่น public key cryptography และ private key cryptography ที่อาจมีความยาวหรือความซับซ้อนของคีย์ที่แสดงด้วยจำนวนบิต นับเป็นสิบหรือเป็นร้อยหรือมากกว่านั้น จุดมุ่งหมายของคีย์รวมทั้งการเข้ารหัสก็คือการรักษาความลับ เมื่อมีความลับก็ย่อมต้องมีบุคคลหรือกลุ่มบุคคลที่ต้องการจะไขความลับด้วยการตีรหัสต่าง ๆ ให้แตก การแก้รหัสในโลกของคอมพิวเตอร์ซีเคียวริตี้จึงเป็นเหมือนการยกกำลังเข้าจู่โจมป้อมปราการ (เช่นการรบในสมัยโบราณ) อันแข็งแกร่งและมิดชิดที่ยากแก่การทะลุทะลวง เมื่อเป็นเช่นนี้การเข้าโจมตีป้อมปราการให้แตกหักจึงต้องอาศัยทั้งกำลังคนและกำลังปัญญา (collaborative effort)

คำว่า "กำลังคน" ในยุคของอินเทอร์เน็ตก็คือการใช้ความสามารถและไหวพริบในด้านคณิตศาสตร์ คอมพิวเตอร์ศาสตร์ ตลอดจนการแบ่งงานกันทำ เช่นในกรณีที่มีปัญหาใหญ่ ๆ ให้ขบคิดนั้น จะแบ่งงานให้แต่ละคนหรือแต่ละทีมที่กระจายอยู่ทั่วโลกว่าใครต้องทำอะไรหรือแก้ปัญหาส่วนไหน แล้วนำคำตอบที่แต่ละคนหรือแต่ละทีมหาออกมาได้มารวมกัน โดยต่างคนต่างส่งคำตอบมายังศูนย์กลางซึ่งเป็นต้นกำเนิดของปัญหาโดยทางอีเมล์ การแก้ปัญหาในทำนองนี้จะเกิดจากการที่มีใครสักคนเกิดอยากรู้อยากเห็นสิ่งที่เป็นความลับและได้มีการเข้ารหัสไว้เช่นในรูปของ prime number หรือ bit-string พวกที่มีความอยากรู้อยากเห็นนี้มักเป็นผู้ที่มีความรู้ด้านคอมพิวเตอร์ศาสตร์หรือคณิตศาสตร์อย่างดีและอยู่ในวัยรุ่น คือจะมีอายุตั้งแต่ในวัยทีนเอจจนถึงประมาณสามสิบเศษ ๆ โดยมักอยู่ตามมหาวิทยาลัย ซึ่งถ้าเป็นในสหรัฐฯ ก็มักเป็นพวกนักศึกษาตามมหาวิทยาลัยใหญ่ ๆ เช่นที่เบิร์กเลย์, MIT ฯลฯ ที่ถือว่าเป็นสถานที่ที่เพียบพร้อมด้วยนักวิชาการและสิ่งสนับสนุน (เช่นศูนย์คอมพิวเตอร์) ทำให้สะดวกในการแก้ปัญหาขนาดใหญ่ที่มีความยากมาก ๆ คืออาจยากจนต้องอาศัยความร่วมมือจากผู้อยากรู้อยากเห็นที่กระจายอยู่ตามมหาวิทยาลัยต่าง ๆ ทั่วโลก การปิดประกาศเพื่อแจ้งรายละเอียดของปัญหาก็กระทำผ่านทางอีเมล์ เพื่อให้กระจายไปทั่วโลก จากนั้นก็จะอาศัยอีเมล์ในการสื่อความระหว่างผู้เป็นเจ้าของปัญหากับบรรดานักแก้ปัญหาที่อยู่ในประเทศต่าง ๆ เพื่อให้มีการรับรู้ความคืบหน้าของการแก้ปัญหา

สิ่งสำคัญที่สุดอย่างหนึ่งในการแก้ปัญหาประเภทที่ต้องถอดรหัสก็คือ การมีอัลกอริธึมทางคำนวณที่มีอานุภาพ เช่น อัลกอริธึมที่ใช้ในการแยกแฟกเตอร์ (factoring algorithms) ซึ่งมักจะมีผู้ค้นคิดเพื่อหาอัลกอริธึมที่ใหม่ ๆ อยู่ตลอดเวลา อันจะทำให้เวลาที่ใช้ในการไขความลับหรือถอดรหัสสั้นลง จนสามารถทำในสิ่งที่แต่ก่อนทำไม่ได้ เพราะยังไม่มีคอมพิวเตอร์ที่เร็วพอ รวมทั้งยังไม่มีอัลกอริธึมที่มีอานุภาพสูงเหมือนปัจจุบัน

ความสามารถขั้นต่อไปที่จำเป็นในการแก้ปัญหาขนาดใหญ่ หรือปัญหาที่มีความยากมาก ๆ ก็คือ การรู้จักแบ่งปัญหาใหญ่ให้เป็นปัญหาย่อย รวมทั้งการสามารถมองเห็นว่าประเด็นหรือหัวใจของปัญหาอยู่ตรงไหน และใครหรือทีมงานใดจะแก้ส่วนใดของปัญหาเพื่อไม่ให้เกิดการซ้ำซ้อนกัน อันเป็นเรื่องที่เจ้าของปัญหา (หรือผู้ตั้งปัญหา) ต้องรู้จักจัดแบ่งและเป็นผู้นำ คือเป็นผู้นำทั้งในทางวิชาการ (เช่น แจกอัลกอริธึมที่ใช้ในการถอดรหัส) และเป็นนักคิด

การบุกรุกเพื่อโจมตีป้อมปราการ (หรือการระดมกำลังเพื่อถอดรหัสโดยผ่านทางอินเทอร์เน็ต) ทำได้สองทางคือ

1. การรุกเข้าไปโจมตีแบบใช้กำลังเพียงอย่างเดียว (frontal attack) คือถ้าจะพูดในแง่ของตัวเลขก็คือการถอดรหัสด้วยวิธีคลำทางชนิดไม่ต้องรู้อะไรมาก การคลำทางเช่นนี้เป็นการคำนวณแบบไล่ไปเรื่อย ๆ เช่น ถ้าเป็นกรณีของรหัสที่มีเลขอยู่ 4 หลัก (XXXX) ก็ไล่ตั้งแต่ 0000 ไปจนเจอตัวเลขที่เป็นรหัส อันต้องใช้เวลาพอสมควร

2. การถอดรหัสหรือล้วงความลับอีกวิธีก็คือการโจมตีที่จุดอ่อน โดยพยายามหาข้อมูลหรือเรียนรู้ข้อผิดพลาดอันเป็นจุดอ่อนของผู้เข้ารหัสให้มากที่สุด รวมไปถึงช่องโหว่หรือความพลั้งเผลอของฝ่ายตรงข้าม ซึ่งมักจะทิ้งร่องรอยบางอย่างไว้ ทำให้การแกะรอยสะดวกขึ้น เช่น การใช้รหัสหรือชื่อที่ผู้อื่นสามารถเดาได้ง่าย

นอกจากทั้งสองข้อนี้ก็เป็นเรื่องของความรอบรู้และไหวพริบที่นักถอดรหัสพึงมี ทั้งหมดนี้ก็เป็นพื้นฐานอย่างกว้าง ๆ ว่าด้วยการโจรกรรมข้อมูลด้วยการถอดรหัสในยุคของอินเทอร์เน็ตที่มักทำงานคนเดียวไม่ได้ แต่ต้องอาศัยทีมงานที่มีความเชี่ยวชาญและอยากรู้อยากเห็น ซึ่งมักกระจายอยู่ตามมหาวิทยาลัยหรือสถาบันค้นคว้าที่มีคอมพิวเตอร์ชนิดอานุภาพสูงติดตั้งอยู่ ส่วนใหญ่มักจะอยู่ในประเทศที่มีความรุดหน้าทางเทคโนโลยีสูงเช่น สหรัฐฯ, ยุโรป

จากนี้ก็จะเข้าสู่กระบวนการในการถอดรหัส เพื่อแสดงให้เห็นความบกพร่องในเรื่องของ

1. การเข้ารหัส เช่นกรณีของ Netscape key

2. การกำหนดความยาว (หรือความยากของรหัส) เช่น RSA-129 ที่แม้จะเป็น public key ที่ซับซ้อนจนเชื่อกันว่าไม่มีใครสามารถถอดรหัสได้ (ความเชื่อเมื่อปี 1977) นั้น ก็ยังมีผู้ถอดรหัสจนสำเร็จในปี 1994 (ดังในรูปที่ 1)

ทำลายปราการ RSA-129

ระบบ RSA เกิดจากผู้คิดค้น 3 ท่าน คือ Ron Rivest, Adi Shamir และ Leonard Adleman ซึ่งถือว่าเป็น public key cryptography ที่เป็นที่นิยมและมีอิทธิพลมากในอดีต ที่เป็นการเข้ารหัสโดยอาศัย key หนึ่งคู่แทนที่จะเป็น key อันเดียว และถือว่าเป็นการรุดหน้าของเทคโนโลยีทางด้านการรักษาความลับให้คนส่วนใหญ่ได้มีโอกาสใช้เทคโนโลยีนี้เมื่อต้องการจะรับหรือส่งข้อมูลข่าวสารด้วยระบบสื่อสารโทรคมนาคมที่ยังไม่มีการให้บริการในการเก็บรักษาความลับ

จุดริเริ่มอันเป็นที่มาของการท้าทายเพื่อให้มีการถอดรหัส RSA-129 นี้เกิดจากนักเขียนคอลัมน์ชื่อดังของวารสาร Scientific American ผู้มีนามว่า มาร์ติน การ์ดเนอร์ (Martin Gardner) ที่ได้นำคำพูดในเชิงปรัชญาของนักประพันธ์ชื่อดังผู้มีนามว่า Edgar Allan Poc มากล่าวเน้นในปี 1977 ในเรื่องของรหัส ดังใจความว่า *"It may roundly be asserted that human ingenuity cannot concoct a cipher which human ingenuity can not rosolve"* ซึ่งสำหรับกาลเวลาต่อมา **มาร์ติน การ์ดเนอร์** เห็นว่าคำพูดของ Edgar Allan Poc อาจไม่จริงเสมอไป

แต่ก่อนที่จะมาถึงปัจจุบันก็จะขอย้อนไปในอดีต (ราว 1977) ว่า เพื่อเป็นการพิสูจน์ความอยู่ยงคงกระพันของระบบ RSA มาร์ติน การ์ดเนอร์ ได้ขอร้องให้ผู้คิดค้นทั้งสามท่านหาวิธีท้าทายผู้ที่คิดจะถอดรหัส ซึ่งก็ได้รับการสนองตอบโดย Rivest ได้สร้างคีย์ขึ้นมาอันหนึ่งที่มีความยาว 129 digits แล้วฝากข้อความอันหนึ่งเข้าไปในรหัสนี้ จากนั้นก็ท้าให้นักถอดรหัสทั้งหลายอ่านข้อความที่เก็บไว้ในรหัสดังกล่าว โดย Rivest, Shamir และ Adleman จะให้รางวัล 100 เหรียญสหรัฐฯ แก่ใครก็ตามที่สามารถอ่านข้อความในรหัสได้ อันเนื่องจาก Rivest ได้เห็นว่าถ้าใครสักคนจะใช้ซุปเปอร์คอมพิวเตอร์ในการแกะโค้ดที่ว่านี้ก็จะต้องใช้เวลาที่นานถึง $40x10^{15}$ ปีกว่าจะถอดรหัสได้ ต่อมาได้มีการแก้ไขจำนวนปีดังกล่าวให้เหลือแค่เพียงราว 2 ถึง 3 ล้านปี เพราะเกิดการผิดพลาดในการคำนวณในเรื่องของระยะเวลา ($40x10^{15}$) ปีในตอนแรก ถึงกระนั้นก็ตาม Rivest ก็ยังแน่ใจว่าระยะเวลาที่ว่าสั้นอยู่แล้ว (2 ถึง 3 ล้านปี) นั้นก็นานพอที่จะทำให้นักถอดรหัสที่มีลมหายใจอยู่ในปัจจุบัน กลายเป็นฟอสซิล (fossilized) ก่อนที่จะสามารถเปิดเผยข้อความใน RSA-129 ได้เป็นผลสำเร็จ ทำให้นักเขียนคอลัมน์ทางวิทยาศาสตร์ชื่อดังเช่น มาร์ติน การ์ดเนอร์ ยิ่งแน่ใจว่าสิ่งที่ Edgar Allan Poc เคยพูดไว้ในอดีตนั้นจะต้องผิดอย่างแน่นอน เพราะการ์ดเนอร์เห็นว่ารหัสที่มีความมั่นคงมากขึ้นเรื่อย ๆ นั้นจะทำให้ความชาญฉลาดของบรรดานักถอดรหัส (ซึ่งมีทั้ง นักศึกษา นักวิจัย นักคณิตศาสตร์ แฮกเกอร์ พวกหัวรุนแรง รวมทั้งผู้ที่ชอบสร้างปัญหาด้วยความอยากรู้อยากเห็นที่กระจายอยู่ทั่วโลก) นับแต่จะลดความสำคัญลงทุกวัน โดยเฉพาะระบบอันแข็งแกร่ง เช่น RSA ซึ่งจะทำให้บรรดานักถอดรหัสตกหลุมพรางและเข้าตาจนได้โดยง่าย

เวลาผ่านไป 15 ปี pablic key encryption ก็ได้แพร่กระจายไปสู่ระบบรักษาความลับต่าง ๆ ที่เป็นผลิตภัณฑ์ด้านซอฟต์แวร์ เช่น RSA Data Security Inc. อันเป็นบริษัทที่มีความเชี่ยวชาญเรื่องระบบ RSA ซึ่งได้ขายลิขสิทธิ์ของเทคโนโลยีในด้านนี้ให้แก่ผู้ผลิตซอฟต์แวร์รายใหญ่ เช่น Lotus และ Microsoft นอกจากนี้ก็มีหนึ่งในบรรดา public key encryption program ที่มีผู้กล่าวถึงมากในสหรัฐฯ นั่นก็คือ Pretty Good Privacy (PGP) ซึ่งผู้เขียนโปรแกรมที่มีนามว่า ฟิล ซิมเมอร์มาน (Phil Zimmermann) ได้แสดงความใจกว้างด้วยการแจกจ่ายโปรแกรมนี้แก่สาธารณะ เพื่อให้คนสองคนที่อยู่ไกลกันสามารถส่งอีเมล์ถึงกันได้โดยผู้อื่นจะแอบอ่านไม่ได้ หรือว่าสามารถลักลอบอ่านอีเมล์ดังกล่าวได้ อย่างไรก็ตาม ในขั้นนี้ผู้เขียนจะขอเจาะจงไปที่การพยายามที่จะถอดรหัสใน RSA-129 เป็นลำดับแรก เนื่องจากมีผู้เห็นว่าจะสามารถถอดรหัสนี้ได้โดยอาศัย factoring algorithm แม้ว่าจะต้องใช้เวลานานนับเดือน รวมทั้งต้องอาศัยความร่วมมือของนักถอดรหัสจากหลายมุมโลกก็ตาม

ความแข็งแกร่งของปราการ เช่น PGP หรือ cryptosystems อื่น ๆ ที่อาศัย RSA public key cryptography นั้นจะอยู่บนรากฐานของหลักเกณฑ์ทางคณิตศาสตร์บางประการ เช่น การคูณเลขสองจำนวนที่มีขนาดใหญ่ที่เป็น prime number เพื่อให้ได้ตัวเลขที่มีขนาดใหญ่มาก ๆ นี่เป็น prime number ที่ทำหน้าที่เป็นคีย์สำหรับใช้ในการเข้าและถอดรหัสสำหรับข้อความ ตัวเลขเช่นนี้จึงเป็นสิ่งที่ยากจนสุดจะพรรณนา สำหรับคนส่วนใหญ่ที่จะล่วงรู้ว่า มาจากผลคูณของตัวเลขสองจำนวนที่ประกอบด้วยอะไรบ้าง ความยากเช่นที่ว่านี้เป็นสิ่งจำเป็นอย่างยิ่งยวด เพราะเป็นการปิดกั้นโอกาสเพื่อให้ใครสามารถแยกแฟกเตอร์ได้ อันจะนำไปสู่การอ่านข้อความที่ขโมยมาได้ บทบาทของ factoring algorithm ในกรณีของ

ตัวเลข 129 ดิจิต จึงเป็นการตะล่อมเพื่อจำกัดความเป็นไปได้ของเลขสองจำนวนที่เป็น prime number ที่เมื่อรวมกันแล้วจะให้เลขที่มีความยาวเท่ากับ 129 หลัก อันเนื่องจากว่าความเป็นไปได้ดังกล่าวมีมากมายเหลือเกิน การจำกัดความเป็นไปได้ให้แคบเข้าจึงเป็นขั้นแรกที่จะนำไปสู่การหาตัวเลขที่เป็นต้นตอที่มีเพียงชุดเดียว ซึ่งการที่จะทำเช่นนี้ได้ก็ต้องมีการติดตามการรุดหน้าของ factoring algorithm เพื่อหาวิธีการคำนวณที่ทันสมัยและมีอานุภาพที่สุดที่จะมาใช้แยกแฟกเตอร์

ในกรณีของ เดเรค แอทกินส์ นั้นเขาได้อาศัยผลการค้นคว้าทางคณิตศาสตร์ของผู้อื่นที่เรียกว่า "double large prime multiple polynomial variation of the quadratic sieve" อันเป็นการหาตัวเลขที่มีความสำคัญจำนวนหนึ่งซึ่งอยู่ในรูปของยูนิตเวกเตอร์ (unit vectors) ซึ่งแอทกินส์เห็นว่าจะช่วยประหยัดเวลาในการค้นหาได้มาก คือภายหลังจากที่สามารถหายูนิตเวกเตอร์ออกมาได้ ผู้ถอดรหัสก็จะสามารถรวมยูนิตเวกเตอร์ดังกล่าวเพื่อคลำทางไปสู่ความสัมพันธ์ทางคณิตศาสตร์ ที่จะทำให้หาตัวเลขที่เป็น prime จำนวนสองตัวที่เป็นต้นกำเนิดของการถอดรหัสได้โดยไม่ยาก

วิธีที่จะเข้าใจแนวความคิดของยูนิตเวกเตอร์นั้นสามารถยกตัวอย่างได้ว่า สมมติว่าเรากำลังค้นหาเข็มนับเป็นจำนวนหลายล้านเล่มในกองฟาง ซึ่งเป็นที่ที่ซ่อนเข็มอีกนับไม่ถ้วนเล่ม โดยเข็มแต่ละเล่มก็จะดีเหมือนเล่มอื่น อันเป็นความเห็นของ **เดเรค แอทกินส์** ผู้มีอายุ 21 ปี (ในปี 1992) และเป็นนักศึกษาด้านวิศวกรรมไฟฟ้าที่ MIT แอทกินส์ได้ให้ความเห็นต่อไปอีกว่า การค้นหาเช่นนี้ไม่ได้มองหาเข็มเล่มใดเล่มหนึ่ง แต่ต้องการที่จะหาเข็มให้มีจำนวนมากพอแล้วผสมผสานเข็มดังกล่าวให้อยู่ในรูปของกรรมวิธีทางคณิตศาสตร์ เพื่อใช้สำหรับแยกแฟกเตอร์ของจำนวนเลข กรรมวิธีนี้เหมาะสำหรับการจู่โจมเพื่อไขความลับโดยอาศัยเน็ตเวอร์กสากลเช่นอินเทอร์เน็ต โดยอาศัยผู้เข้าร่วมจู่โจมเป็นจำนวนมากที่กระจายอยู่ในประเทศต่าง ๆ อันเนื่องจากการที่แต่ละคนสามารถอุทิศเวลาของคอมพิวเตอร์มาแก้ปัญหาเดียวกัน ในกรณีของ RSA-129 นี้นักถอดรหัสต้องการยูนิตเวกเตอร์ราวครึ่งล้านโดยไม่ได้ต้องการที่จะให้ยูนิตเวกเตอร์ที่มีความเป็นไปได้ทุกตัวให้มาทำหน้าที่แยกแฟกเตอร์จำนวนเลข อันหมายถึงการต้องการกลั่นกรองเอาเฉพาะยูนิตเวกเตอร์ที่มีศักยภาพในการนำไปสู่การแยกแฟกเตอร์เท่านั้น เพื่อมาเก็บไว้ที่ MIT อันเป็นที่อยู่ของแอทกินส์ผู้เป็นเจ้าของความคิดที่จะแกะรหัส RSA-129 โดยอาศัยไพร่พลเกือบทั่วโลก ยกเว้นทวีปแอนตาร์กติก

การระดมพลเพื่อถอดรหัส RSA-129

ในปลายฤดูร้อนของปี 1993 แอทกินส์และเพื่อนสนิทที่ MIT ก็ได้มีซอฟต์แวร์อยู่ในมือที่จะใช้สำหรับล่ายูนิตเวกเตอร์ ซึ่งจำเป็นต้องเกณฑ์ผู้ที่จะอาสาสมัครเพื่อช่วยกันค้นหายูนิตเวกเตอร์ โดยการส่งข่าวผ่านทาง mailing lists และ newsgroup พร้อมด้วยการแจกซอฟต์แวร์โดยผ่านทางอินเทอร์เน็ต ดังนั้นใครก็ตามที่มีคอมพิวเตอร์และสามารถโหลดซอฟต์แวร์ของแอทกินส์เข้าไปในเครื่อง ก็จะสามารถช่วยการค้นหายูนิตเวกเตอร์ที่จะนำ

ไปสู่การถอดรหัสได้ ผู้ร่วมอาสาสมัครเพื่อช่วยแฮทกินส์มีถึง 1,600 รายจากทั่วโลก โดยมีผู้ให้ความร่วมมือทุกทวีปยกเว้นแอนตาร์กติก ส่วนในแง่ของคอมพิวเตอร์ที่ช่วยในการถอดรหัสครั้งนี้มีตั้งแต่พีซีธรรมดาจน MasPar ซุปเปอร์คอมพิวเตอร์ของ Bellcore ที่มีโปรเซสเซอร์ 16,000 ตัว ซึ่งถือว่าเป็นคอมพิวเตอร์ที่มีอานุภาพติดอันดับโลก

จากกันยายน 1993 ถึงเมษายน 1994 การทดลองเพื่อถอดรหัส RSA-129 ได้ใช้พละกำลังด้านคอมพิวเตอร์หมดไป 5,000 mips-ปี โดยที่หนึ่ง **mips-ปี** จะเท่ากับคอมพิวเตอร์ที่ประมวลผลได้หนึ่งล้านอินสตรัคชันต่อวินาที ซึ่งทำงานอยู่อย่างต่อเนื่องเป็นเวลานานหนึ่งปี แฮทกินส์และผู้ร่วมทีมเห็นว่าน่าจะได้ยูนิตเวกเตอร์มากพอที่จะทำการคำนวณเพื่อแยกแฟกเตอร์ของ prime number ที่มีความยาว 129 ดิจิตได้แล้ว โดยในขั้นแรกจะต้องนำยูนิตเวกเตอร์ (หรือเข็ม) ทั้งหมดที่รวบรวมได้มาจัดให้อยู่ในรูปของแมตริกซ์ (a very sparce matrix) จากนี้ก็ต้องอาศัยคอมพิวเตอร์ที่มีอานุภาพที่สูงมาก ๆ มาอ่านข้อมูลจากแมตริกซ์เข้าไปแล้วทำการคำนวณเพื่อสลายตัวเลขในแมตริกซ์ดังกล่าวให้เหลือแค่เพียง prime number เพียงสองตัว ซึ่งแฮทกินส์ก็ได้ส่งผลของการรวบรวมยูนิตเวกเตอร์จากที่มีผู้ส่งมาให้ทางอีเมล์ ซึ่งมีปริมาณมากถึง 400 เมกะไบต์ที่เก็บในเทป ไปให้นักคณิตศาสตร์ที่เคยรู้จักและคุ้นเคย ผู้มีนามว่า Argen Lenstra ซึ่งทำงานอยู่ที่ Bellcore เพื่อขอความร่วมมือในการใช้ MasPar ซุปเปอร์-คอมพิวเตอร์ในการคำนวณหา prime number สองจำนวนจากแมตริกซ์ดังกล่าว

การคำนวณดังกล่าวได้ใช้เวลาถึง**สองวัน** ก่อนที่จะได้คำตอบดังแสดงไว้ในรูปที่ 1 อันเป็นคำตอบที่ปรากฏออกมาเมื่อวันที่ 26 เมษายน 1994 ซึ่งได้หมดเวลาไป 8 เดือน นับจากวันเริ่มต้นการไล่ล่าเพื่อรวบรวมยูนิตเวกเตอร์ ซึ่งจากการอาศัยคีย์ดังในรูปที่ 1 ก็ทำให้แฮทกินส์อ่านข้อความที่เข้ารหัสไว้ได้โดยมีใจความว่า **"The magic words are squeamish ossifrage."** ซึ่งเมื่อได้ทราบข่าวนี้ Rivest ก็ยอมรับว่าการที่มีผู้สามารถถอดรหัสของเขาได้ก็เพราะเทคโนโลยีในเรื่องของการแยกแฟกเตอร์ได้ก้าวหน้าไปอย่างรวดเร็ว จนทำให้อัลกอริธึมที่เร็วมาก ๆ เกิดใหม่ จนต้องมีการติดตามอยู่ทุกขณะ โดยเฉพาะสำหรับผู้ที่สนใจในการเข้าและ/หรือถอดรหัส ซึ่งเมื่อมีการผนวกเทคโนโลยีดังกล่าวกับคอมพิวเตอร์ที่เร็วอย่างสุด ๆ ในอนาคตอันใกล้เช่นควอนตัมคอมพิวเตอร์ (quantum computers) ก็แทบจะไม่มีรหัสอันใดในโลกที่มนุษย์จะถอดไม่ได้ ทั้งหมดนี้ก็เป็นผลงานของเดเรค แฮทกินส์กับทีมงาน MIT และอาสาสมัครทั่วโลก

จากนี้ก็จะพูดถึงผลการถอดรหัสของรายอื่น ๆ ที่อาศัยหลักของ participatory cryptanalysis เหมือนกรณีของแฮทกินส์ดังเช่น Hal Finney ซึ่งเป็นโปรแกรมเมอร์ที่อยู่ใน Santa Barbara แคลิฟอร์เนียและเป็นผู้มีส่วนร่วมพัฒนา PGP แต่ไม่เห็นด้วยกับการที่รัฐบาลสหรัฐฯ ได้มีมาตรการในการจำกัดขนาดของคีย์สำหรับรหัสที่ใช้ในผลิตภัณฑ์สำหรับการส่งออก ซึ่งมีความยาวแค่ 40 บิตเท่านั้น ทำให้ผู้ผลิตซอฟต์แวร์ในด้านนี้ต้องหาทางออก เช่น ด้วยการสร้างคีย์ที่มีสองเวอร์ชันด้วยกัน คือเวอร์ชันที่ใช้ในสหรัฐฯ จะเป็นแบบ long keys และเวอร์ชันที่ส่งไปจำหน่ายในต่างประเทศจะเป็นแบบ short keys ทำให้มีผู้ไม่เห็นด้วย จนต้องการพิสูจน์ให้โลกเห็นว่า 40 bit crypto นั้นสามารถถูกตีแตกได้โดยมือสมัครเล่น หนึ่งในผู้ที่ไม่เห็นด้วยก็คือ ฮัล ฟินนีย์ (Hal Finney) รวมทั้งบรรดา cypherpunks ที่อยู่ในประเทศอื่น ๆ นอกจากสหรัฐฯ ดังนั้นเมื่อฟินนีย์ได้ออกมาโฆษณาให้มีการต่อต้านในเรื่องของ short keys จึงมีผู้เห็นด้วยอย่างมาก

ปลุกระดมเพื่อคัดค้าน 40 bit crypto

วิธีการต่อต้านในรูปของการโฆษณาชวนเชื่อของฮัล ฟินนีย์ในเรื่องของ short key versions ก็คือการสร้างรายการที่เป็นดัมมี่ (dummy transaction) ขึ้นมารายการหนึ่ง ภายใน Netscape และอาศัยเวอร์ชันของคีย์ที่ใช้สำหรับส่งออกเป็นเครื่องมือในการเข้ารหัส จากนั้นก็ทำการท้าทายเพื่อร่วมขุทธจักรหรือบรรดา cypherpunks ด้วยการประกาศในอินเทอร์เน็ตให้มีการแข่งกันถอดรหัสในรายการที่เขาเป็นผู้เข้ารหัสไว้ ทำให้เกิดการวิ่งแข่งกันว่าใครจะเป็นรายแรกที่สามารถตีรหัสที่เป็น expert level security ของ Netscape ให้แตกได้และเพื่อเป็นการตอบโต้เจ้าหน้าที่ของสหรัฐฯ ที่ให้ความมั่นใจกับคนทั่วไปว่าซีเคียวริตี้ในระดับนี้เป็นสิ่งที่พอเพียงสำหรับประเทศ

```
We are happy to announce that RSA-129 =
114381625757888867669235779976146612010218296
721242362562561842935706935245733897830597l2
3563958705058989075147599290026879543541 =
3490529510847650949147849619903898133417764 63
849338784399082057 7 * 327691329932667095499 61
988190834461413177642967992942539798288533
```

รูปที่ 1 แสดงผลของการถอดรหัสด้วยฝีมือของ เดเรค แฮทกินส์ (Derek Atkins) แห่ง MIT พร้อมด้วยนักคอมพิวเตอร์สมัครเล่นที่อยู่ในประเทศต่าง ๆ รหัสดังกล่าวอยู่ในรูปของ RSA คีย์ อันเป็น prime number ที่มีความยาวเท่ากับ 129 digit การร่วมกันถอดรหัสนี้ได้ใช้เวลาประมาณ 8 เดือน และสามารถไขความลับได้ในวันที่ 26 เมษายน 1994 ตัวเลขที่แสดงนี้เป็นประกาศของ เดเรค แฮทกินส์ เพื่อให้โลกรู้ถึงความสมัครสมานในการแก้ปัญหาในหมู่นักคอมพิวเตอร์รุ่นครู และอาจเป็นไปได้ว่าสักวันหนึ่งนักคอมพิวเตอร์สมัครเล่นก็ทำเช่นนี้ได้ในรูปของการช่วยกันคนละไม้คนละมือ

อื่นที่อยู่นอกสหรัฐฯ อันเป็นชนวนเหตุที่ยั่วยุให้นักคอมพิวเตอร์เช่น ฟินนีย์และ cypherpunks อื่น ๆ ต้องออกมาแสดงฝีมือว่าคีย์ที่มีความยาวแค่ 40 บิตนี้จะให้ซีเคียวริตี้ได้สักแค่ไหน

ผู้เข้าร่วมขบวนกับฮัล ฟินนีย์เป็นรายแรกก็คือ นักศึกษาด้านคอมพิวเตอร์ศาสตร์แห่งมหาวิทยาลัยเอ็กซีเตอร์ในอังกฤษ ซึ่งมีอายุ 25 ปี และมีชื่อว่า อะดัม แบค (Adum Back) แบคเป็นหนึ่งในจำนวนนักศึกษาอีกหลาย ๆ คนที่อ่านประกาศในอินเทอร์เน็ตในเรื่องของ cypherpunk list เพื่อหาความรู้และข่าวสารในเรื่องของรหัสวิทยา (cryptography) และเพื่อเป็นการเตรียมพร้อมในเรื่องของการร่วมกันถอดรหัสแบบเป็นกลุ่ม (group crack) ที่ทำให้แบคกับเพื่อน ๆ ร่วมกันเขียนโปรแกรมสั้น ๆ ขึ้นมาใช้สำหรับการกระจายกำลังในการถอดรหัสสำหรับในกรณีที่อาจได้รับการขอแรงดังเช่นการประกาศของฮัล ฟินนีย์

ความตั้งใจในขั้นแรกของแบคก็คือการแบ่งปัญหาของฟินนีย์ โดยแบ่ง Keyspace ที่เกิดจากปัญหานี้ออกเป็นส่วน ๆ เพื่อให้นักถอดรหัสช่วยกันแก้ปัญหาอันเป็นการแบ่งงานที่แบคได้แจ้งให้ผู้ที่เกี่ยวข้องรู้โดยผ่านทางเวบเพจของตน แต่ก็ได้มีโปรแกรมเมอร์ชาวออสเตรเลียคนหนึ่งที่ชื่อว่า อีริค ยัง (Eric Young) ได้เสนอตัวว่าต้องการจะรับปัญหาไปแก้ครึ่งหนึ่งโดยจะเลือกเอาครึ่งหลัง (the second half of possible keys) แผนแบ่งแยกปัญหาเป็นส่วนย่อยของแบคจึงต้องล้มเลิก เพราะอาสาสมัครแต่ละรายอยากจะแก้ปัญหาที่มีขนาดใหญ่พอสมควร เช่นกรณีของอีริค ยัง

นอกจากนี้ก็ยังมีโปรแกรมเมอร์ชนิดฉายเดี่ยวอีกรายที่มีอายุ 24 ปี เป็นชาวอเมริกันชื่อ เดวิด ไบเออร์ (David Byers) ซึ่งกำลังเรียนอยู่ที่มหาวิทยาลัย Linkoping ในสวีเดน ที่ต้องการจะรับผิดชอบแก้ปัญหาครึ่งแรก (the first half of the keyspace) เพราะเห็นว่ามหาวิทยาลัยของตนมีคอมพิวเตอร์ที่มีความเร็วอันฉกาจที่เรียกว่า MasPar MP-1 ซึ่งสามารถค้นหาสิ่งที่อยู่ใน keyspace ได้ด้วยความเร็ว 1.5 ล้านคีย์ต่อวินาที อีริค ยัง ได้วิ่งโปรแกรมที่เขาเขียนขึ้นมาใน MasPar โดยใช้เวลาคอมพิวเตอร์ครั้งละ 6 ชั่วโมงเป็นเวลาหลายวัน แต่ก็ยังไม่ได้ผลอะไรที่น่าพอใจ ที่พูดมาทั้งหมดนี้น่าจะเป็นช่วงเวลาหลังปี 1994 อันเป็นเวลาหลังจากที่ได้มีผู้พิชิต RSA-129 ได้สำเร็จ อันเป็นการกรุยทางเพื่อให้เกิดการตื่นตัวในการรณรงค์เพื่อให้ช่วยกันถอดรหัสในผลิตภัณฑ์หรือในนโยบายของรัฐที่บรรดา cypherpunks เห็นว่าน่าจะไม่ใช่ปรากการในด้านซีเคียวริตี้ที่ใช้การได้ และในขณะนี้ยังไม่มีอะไรเกิดขึ้นกับการควานหาคีย์ที่เป็นตัวรหัสของเดวิด ไบเออร์ ก็ได้มีนักวิทยาศาสตร์ด้านคอมพิวเตอร์อีกรายในฝรั่งเศสที่ต้องการแก้ปัญหาทั้งหมดที่เกิดจากการชี้ชวนของฟินนีย์ด้วยตนเอง

นักวิทยาศาสตร์ที่ทำงานในฝรั่งเศสผู้นี้มีชื่อว่า ดาเมียน โดลิเก้ (Damien Doligey) ที่อยู่ในวัย 27 และทำงานด้านวิจัยอยู่ที่ INRIA อันเป็นห้องทดลองด้านคอมพิวเตอร์ของรัฐบาลฝรั่งเศส สิ่งแรกที่โดลิเก้ทำก็คือการเขียนโปรแกรมเล็ก ๆ ขึ้นมาอันหนึ่งเพื่อสั่งให้คอมพิวเตอร์ค้นหาคีย์ที่มีศักยภาพ พร้อมกับนำโปรแกรมนี้ไปปรับปรุงเพื่อใช้วิ่งในคอมพิวเตอร์ต่าง ๆ ที่อยู่ใน INRIA เน็ตเวอร์ก และที่อยู่ในมหาวิทยาลัยข้างเคียงเพื่อที่จะค้นหาคำตอบออกมาให้เร็วที่สุด การค้นหาคีย์ของโดลิเก้ทำไปด้วยความเร็วเฉลี่ย 10,000 คีย์ต่อวินาที โดยเริ่มจากปลายสุดของ keyspace แล้วคำนวณย้อนหลัง เพราะเห็นว่าน่าจะมีโอกาสอย่างสูงในการพบคีย์ที่เป็นตัวจริง อันนี้ก็เป็นเวลาในช่วงวันที่ 11 สิงหาคม 1995 และเป็นวันศุกร์ ซึ่งหลังจากนี้โดลิเก้ก็ลาพักร้อนเป็นเวลา 4 วัน ในระหว่างการลาหยุดโดลิเก้ได้ใช้คอมพิวเตอร์จากที่บ้านในการตรวจสอบการคำนวณของเวอร์กสเตชันที่อยู่ใน INRIA และได้แลเห็นว่าเวอร์กสเตชันที่ INRIA ได้เจอคีย์เข้าแล้ว แต่ก็ไม่ได้รีบร้อนอะไร เพราะอยากจะใช้เวลาพักผ่อนช่วงการลาหยุด 4 วันให้เต็มที่

ในส่วนของนักถอดรหัสซึ่งมีชาวอังกฤษ/ออสเตรเลีย/สวีดิชนั้น MasPar คอมพิวเตอร์ที่เดวิด ไบเออร์ ใช้อยู่สามารถค้นพบคีย์ที่ต้องการและได้ส่งคีย์ดังกล่าวไปให้แบคที่อังกฤษ แต่แบคก็ไม่สามารถจะอ่านข้อความที่ฟินนีย์เข้ารหัสไว้ได้หมด คืออ่านได้เพียงครึ่งแรกของข้อความ เพราะได้เกิดข้อผิดพลาดขึ้นเพียงเล็กน้อย

ผู้ที่สามารถถอดรหัสและอ่านข้อความที่ฟินนีย์เขียนซ่อนไว้ได้สำเร็จเป็นรายแรกคือโดลิเก้ และได้ปิดประกาศการค้นพบของตนให้บรรดา cypherpunks ทราบ ข้อความที่เป็น coded message ของฟินนีย์มีดังนี้

"Mr. Cosmic Kumquat, SSL Trusters Inc. 1234 Squeamish Ossifrage Road, Anywhere, NY 12345 (USA)"

การถอดรหัสเพื่ออ่านข้อความในกรณีของโดลิเก้นี้ได้ใช้เวลาเป็นจำนวน **64 mips-ปี** เพียงเพื่อที่จะต่อสู้กับ 40 บิตคีย์ แต่ถ้าเป็นเวอร์ชันที่ใช้ในสหรัฐฯ ที่มีความยาวถึง 128 บิต นั้น โดลิเก้ได้ยอมรับว่าถ้ามีคอมพิวเตอร์ 1,000 ล้านเครื่อง และแต่ละเครื่องคำนวณได้เร็วกว่าคอมพิวเตอร์ที่โดลิเก้ใช้อยู่ 1 ล้านเท่า ก็ยังคงต้องใช้เวลานานถึง 6,000 ล้านปีกว่าจะถอดรหัสนี้ได้ (128 บิต)

รูปที่ 2
เดวิด แวกเนอร์ (David Wagner) ซึ่งเป็นหนึ่งในสองนักศึกษาที่ UC Berkeley ที่ฉวยโอกาสจากช่องโหว่ในด้านซีเคียวริตี้ของ Netscape จนสามารถล้วงความลับในกุญแจรหัสได้สำเร็จ

เดวิด แวกเนอร์ ที่เบิร์กเลย์

ผู้ที่ให้ความสนใจในเรื่องของคอมพิวเตอร์ซีเคียวริตี้อีกกลุ่มหนึ่งที่น่านำมากล่าวในที่นี้ก็คือนักศึกษาขั้นบัณฑิตวิทยาลัยของเบิร์กเลย์ที่มีอายุ 21 ปีและมีนามว่าเดวิด แวกเนอร์ (David Wagner) ที่มีเพื่อนที่พึ่งมารู้จักกันที่เบิร์กเลย์ และมีความสนใจในเรื่องเดียวกัน นั่นก็คือนักศึกษาในบัณฑิตวิทยาลัยชาวแคนาดาวัย 22 ผู้มีนามว่าไอแอน โกลด์เบิร์ก (Ian Glodberg) เมื่อทั้งคู่มาพบกันที่เบิร์กเลย์ด้วยวัยอันไล่เลี่ยกัน เรียนในบัณฑิตวิทยาลัยเหมือนกัน สนใจในเรื่องของซีเคียวริตี้ และมีอะไรหลาย ๆ อย่างที่คล้าย ๆ กัน โดยเฉพาะการได้รับอิทธิพลจากผลการถอดรหัสของบรรดา cypherpunk ดังได้กล่าวในตอนต้น จนทำให้ต้องกอดคอเพื่อกระโดดเข้ามาในโลกของนักถอดรหัส ที่สำคัญก็คือว่า ในเดือนกันยายนของปี 1995 ในขณะที่เดวิด แวกเนอร์นั่งอยู่หน้าคอมพิวเตอร์ประจำตัวที่มหาวิทยาลัยเพื่อจ้องมองการทำงานของซีเคียวริตี้โปรแกรมของ Netscape ก็ได้พบในสิ่งที่ทำให้ประหลาดใจหลายอย่าง อันเนื่องมาจากการทำงานของโปรแกรมดังกล่าว จนทำให้ระงับความสงสัยไว้ไม่ได้ เพราะยังมีความฝักใฝ่ในอันที่จะนำจุดบกพร่องใน Netscape มาตีแผ่ (ด้วยความหวังดี) ให้จงได้

อย่างไรก็ตาม การเข้าตีปราการที่เป็น crypto ของ Netscape แบบตรงไปตรงมาที่ใช้แต่เพียงพละกำลังทางคอมพิวเตอร์โดยไม่ได้ใช้เทคนิคอื่น ๆ เข้ามาช่วยมากเท่าที่ควร เมื่อเป็นเช่นนี้การจู่โจมเพื่อล้วงความลับในรูปของ brute force attacks จึงไม่ใช่วิธีที่เดวิดและเพื่อนจะใช้ คือต้องหาหนทางอื่นที่ดีกว่า นั่นก็คือเลือกจู่โจมไปที่ช่องโหว่หรือความบกพร่องของ Netscape ด้วยการมุ่งความสนใจที่ plaintext หรือร่องรอยที่ได้มีการทิ้งไว้ให้ผู้ที่ช่างสังเกตสามารถแกะรอยเพื่อติดตามอะไร ๆ ต่อไปจนถึงต้นทาง อันเนื่องจากว่าบุคคลที่สร้าง Netscape ขึ้นมาให้เป็นผลิตภัณฑ์ที่ขายไปได้ทั่วโลกนั้นก็เป็นมนุษย์เดินดินที่มีโอกาสที่จะทำอะไรที่ผิดพลาดหรือประมาทได้ไม่ต่างจากบุคคลอื่น

การหาจุดอ่อนใน Netscape ในกรณีของเดวิด แวกเนอร์ จึงได้อาศัยหลักว่าจะมีที่ไหนบ้างภายในโปรแกรมต่าง ๆ ที่ทำหน้าที่ในด้านซีเคียวริตี้ที่ควรเข้าไปตรวจสอบความแข็งแกร่งเป็นอันดับแรก ซึ่งในที่สุดก็พบว่ามีอยู่ส่วนหนึ่งของโค้ดที่ทำหน้าที่เป็นอินสตรัคชันสำหรับ Psendo-Random Number Generator (PRNG) ของ Netscape ที่ถือว่าเป็นส่วนสำคัญของระบบเข้ารหัส โค้ดส่วนนี้จะแปลงเนื้อหาหรือข้อความที่ต้องการรักษาความลับให้เป็นอักขระที่อ่านไม่รู้เรื่อง อันเป็นการเข้ารหัสที่เป็นไปอย่างมีขั้นตอน นอกจากนี้ก็ยังมีความจริงอยู่ว่า การไม่เป็น random อย่างแท้จริงของ PRNG จึงเป็นจุดอ่อนที่นักถอดรหัสที่มีความเชี่ยวชาญสามารถที่จะเข้าไปแกะช่องย่องเบาได้โดยไม่ยาก ดังนั้นการมี PRNG ที่แข็งแกร่งจึงเป็นสิ่งสำคัญ อันหมายถึงการมีกลไกบางอย่างที่จะหมุนกงล้อของตัวอักษรและตัวเลขเพื่อให้เกิดความเป็น random ให้มากที่สุด PRNG ที่ดีจะใช้ตัวเลขหรือ seed ที่ผู้อื่นคาดคะเนไม่ได้ ตัวเลขนี้เป็นจุดเริ่มของกระบวนการ randomization อันจะต่างกับการทอดลูกเต๋า เพราะการทำงานของคอมพิวเตอร์ในแต่ละครั้งหรือในแต่ละจุดเริ่มต้นจะเหมือนกันหมด จึงจำเป็นต้องหาทางในการเริ่มกระบวนการด้วย seed ที่ศัตรูไม่สามารถเดาได้ว่าเป็นอะไร วิธีในการเลือก seed จึงมักต้องอาศัยสถิติที่อยู่นอกตำรา เช่น ดูจากตำแหน่งของเม้าส์ เป็นต้น แต่ Netscape ได้มองข้ามวิธีเช่นนี้โดยไปยึดติดกับสิ่งที่มีความตายตัวดังเช่นที่แวกเนอร์สังเกตเห็น กล่าวคือ PRNG ของ Netscape ทำงานโดยอาศัยหลักของเวลาในวันหนึ่ง ๆ (time of day) พร้อมด้วย identification ที่มีสองแบบคือ Process ID และ Parent ID ซึ่งแวกเนอร์เห็นว่าเป็นทางไปสู่ความหายนะ

การค้นหาส่วนแรกของ seed แทบไม่ต้องคิดอะไรมาก นั่นก็คือวิ่งโปรแกรมไปตามเวลาของวันโดยใช้เวลาต่าง ๆ กัน (run through varions times of day) จากนี้ก็มาถึงส่วนอื่น ๆ ของ seed (ID) ซึ่งในหลาย ๆ กรณีจะสามารถสกัดจับได้อย่างไม่ยาก โดยเฉพาะถ้าใครสักคนใช้เซอร์ฟเวอร์ร่วมกับผู้อื่น ดังเช่นที่มีปรากฏการณ์ในสภาพแวดล้อมที่เป็นอินเทอร์เน็ตหรือในมหาวิทยาลัยเช่น UC Berkeley คือถ้าผู้จู่โจมมีบัญชีการใช้คอมพิวเตอร์ในคอมพิวเตอร์ของท่านก็จะทำให้ง่ายขึ้น อันเป็นความเห็นของไอแอน โกลด์เบิร์ก ซึ่งได้ให้ความเห็นต่อไปว่า การจะแกะรอย IDs ของ

ผู้ใช้คอมพิวเตอร์ในกรณีของ Netscape เป็นของที่ทำได้ไม่ยากนัก แม้ว่าผู้จู่โจมไม่มีทางที่จะเข้าถึงคอมพิวเตอร์ที่มี IDs ของผู้ใช้รายต่าง ๆ บรรจุอยู่ก็ตาม อันเนื่องจากว่าสิ่งที่เป็นรหัสของ IDs จะมีความยาวเพียง 15 บิต ที่ไม่ยากเกินกว่าที่จะจู่โจมแบบใช้แต่เพียงพละกำลังของคอมพิวเตอร์เพียงอย่างเดียว (brute force attack) สรุปได้ว่าความผิดพลาดของ Netscape ก็คือการใช้ระบบซีเคียวริตี้ที่ยึดติดกับสิ่งที่ผู้อื่นสามารถสังเกตหรือคาดคะเนได้ อันถือว่าไม่ได้ใช้หลักของ randomization อย่างแท้จริง

แวกเนอร์และโกลด์เบิร์กได้เริ่มเขียนโปรแกรม (หลังกันยายน 1995) โดยนำเอาจุดต่าง ๆ ที่เป็นช่องโหว่ของ Netscape เข้ามาพิจารณา โดยทั้งคู่จะใช้เวลาในวันหยุดสุดสัปดาห์ในการค้นคว้าและเขียนโปรแกรม และใช้เวลาในตอนกลางคืนของวันอาทิตย์เพื่อทดสอบโปรแกรมที่เขียนขึ้น โปรแกรมทั้งหมดที่แวกเนอร์และโกลด์เบิร์กเป็นผู้เขียนขึ้นนี้ได้หวังที่จะเจาะเข้าไปในส่วนที่เป็นช่องโหว่ขนาดใหญ่ในการทำงานของ Netscape จนทำให้ทั้งคู่สามารถค้นหาคีย์ (key) ได้โดยใช้เวลาน้อยกว่าหนึ่งนาที ซึ่งโกลด์เบิร์กก็ได้นำผลของการถอดรหัสจนพบคีย์ลงประกาศในmailing lists ของบรรดา cypherpunks ในคืนวันเดียวกับที่ไขความลับของ Netscape ได้สำเร็จ อันทำให้ผู้ที่รับผิดชอบด้านซอฟต์แวร์ซีเคียวริตี้ต้องร้อน ๆ หนาว ๆ ไปตาม ๆ กัน โดยเฉพาะกับการถอดรหัสที่ไม่ต้องอาศัยเน็ตเวอร์กของเวอร์กสเตชันหรือซุปเปอร์-คอมพิวเตอร์ แต่ได้อาศัยอุปกรณ์แค่เพียง Pentium แมชีนที่เป็นธรรมดา ๆ โดยใช้เวลาในการถอดรหัสไม่กี่นาที

การพบข้อบกพร่องครั้งนี้ได้มีผลให้ Netscape รีบแก้ปัญหาด้วยการเข็นเวอร์ชันใหม่ของ Navigator ออกสู่ตลาดโดยเร็ว เพื่อรักษาภาพพจน์ของบริษัท จนถึงกับตั้งรางวัลสำหรับผู้ที่สามารถพบจุดอ่อนของซีเคียวริตี้ในซอฟต์แวร์ของบริษัทนี้ ความพยายามของนักคอมพิวเตอร์รุ่นเยาว์ในอันที่จะล้วงความลับของระบบซีเคียวริตี้ด้วยการรวมกลุ่มกันถอดรหัสในรูปของ collective code breaking ไม่ได้สิ้นสุดเพียงแค่นี้ แต่จะคงดำเนินอยู่ต่อไปจนกว่าจะมีปัญหาอื่นที่ใหญ่กว่านี้เกิดขึ้นมาดึงความสนใจบรรดา cypherpunks ที่ส่วนมากมักไม่ได้ทำไปในแง่ของโจรกรรม แต่จะเป็นไปในทางดีเพื่อก่อด้วยความหวังดี ตามวิสัยของคนที่มีความฉลาดปราดเปรื่องสูงที่มองโลกในแง่ดี

เดเรค แอทกินส์ กับ PGP

ผู้เขียนได้เคยพูดถึงเรื่องของ public key encryption program ที่เรียกว่า PGP ในตอนต้น อันเป็นผลงานของ Phil Zimmermann โดยมีนักศึกษาวัย 21 ที่ชื่อว่า เดเรค แอทกินส์ (Derek Atkins) แห่ง MIT เป็นผู้ให้ความสนใจในแง่ของความปลอดภัยของ PGP ในตอนแรกที่เป็นโปรแกรมนี้ ซึ่งก็ในราวปี 1992 อันเป็นขณะที่แอทกินส์ยังเรียนวิศวกรรมไฟฟ้าอยู่ โดยได้มีความคิดร่วมกับเพื่อน ๆ ที่จะตีรหัสของโปรแกรมนี้ให้แตก จนถึงขั้นรวบรวมสมัครพรรคพวก เช่น Michael Graff ซึ่งเรียนอยู่ที่ Iowa State U. และ Panl Leyland จากมหาวิทยาลัยอ็อกซ์ฟอร์ด เพื่อร่วมกันถอดรหัสโดยอาศัยทรัพยากรด้านคอมพิวเตอร์ที่กระจายอยู่ตามมหาวิทยาลัยที่ทั้งสามเรียนอยู่ รวมทั้งอาศัยการทุ่มเทอย่างเป็นบ้าเป็นหลังที่คิดว่าจะนำไปสู่การถอดรหัสใน PGP ได้สำเร็จ

วิธีการในการจู่โจม PGP ที่แอทกินส์และพรรคพวกคิดจะใช้ในขณะนั้นก็คือ factoring เทคนิค แต่ได้คิดขัดปัญหาตรงที่ว่าตัวเลขต่าง ๆ ที่ใช้เป็น keys ของ PGP นั้นมีขนาดใหญ่มากจนแม้ว่าจะพึ่งกำลังคำนวณจากทั้งเน็ตเวอร์ก (อินเทอร์เน็ต) ก็คงจะแยกแฟกเตอร์ไม่สำเร็จ จนต้องหันไปจู่โจม RSA-129 แทน โดยทำตามคำแนะนำของนักคณิตศาสตร์มีชื่อผู้หนึ่งที่ทำงานที่มี Bellcore และมีนามว่า Arjen Lenstra ที่เป็นผู้สอนให้แอทกินส์อาศัยพละกำลังทางคำนวณของคนหมู่มากที่ใช้อินเทอร์เน็ต เป็นเครื่องมือในการตี RSA-129 ให้แตก ซึ่งแอทกินส์และสาวกจากทั่วโลก (1,600 ราย) ก็ทำได้สำเร็จเมื่อ 26 เมษายน 1994

จากนี้ก็จะขอกลับมาที่ PGP ซึ่งได้มีผู้สัมภาษณ์ Phil Zimmermann เป็นการส่วนตัวว่า โปรแกรมของเขาจะถูกใครสักคนตีแตกได้ไหมในอนาคต ซึ่ง Phil ก็ได้ตอบว่า เขาเชื่อว่าการจู่โจมเพื่อตี PGP ให้แตกนั้นอาจไม่มุ่งไปที่ขนาดของคีย์ (key size) อย่างไรก็ตาม โปรแกรมเช่น PGP นี้อาจมีอันตรายหากผู้จู่โจมใช้วิธีอื่น ผู้ที่สัมภาษณ์ในกรณีนี้มีชื่อว่า Robert Morris Sr., (เป็นนักวิทยาศาสตร์ชั้นผู้ใหญ่ของ National Security Agency ของสหรัฐฯ) ก็ไม่ได้แสดงอากัปกิริยาอะไรออกมาเพื่อให้รู้ว่า NSA ได้ถอดรหัส PGP จนสำเร็จหรือไม่อย่างไร คือยังคงปล่อยให้เป็นปริศนา

สรุป

นิทานในเรื่องของระบบซีเคียวริตี้ของคอมพิวเตอร์เน็ตเวอร์ก จึงน่าจะสอนได้ว่าความปลอดภัยที่สมบูรณ์แบบเป็นเพียงภาพลวงตา เพราะแม้แต่นักศึกษาวัยรุ่นที่รู้จักคิดและรู้จักวางแผนระดมพล ก็สามารถคิดการใหญ่เพื่อตีรหัสที่มีชื่อของโลกให้แตกได้ แม้ว่าจะใช้เวลานานนับเดือนก็ตาม ฝีมือของเด็กเช่น เดเรค แอทกินส์ อาจสู้นักวิทยาศาสตร์คอมพิวเตอร์ของ NSA ไม่ได้ในเรื่องของชั่วโมงบิน แต่ความสามารถของเด็กและมือสมัครเล่นที่ชอบที่จะไฝ่เรียนรู้นั้นเป็นสิ่งที่ไม่ควรมองข้ามเป็นอย่างยิ่ง โดยเฉพาะในแง่ของความพยายาม